



RISK BASED AUDITING WORKSHOP

**(Enterprise-Wide Risk Management,
Corporate Governance Risk, Strategic Risk &
Technology Risk)**

Presented By:

CPA IBARHIM J.MAROA

25TH-26TH AUGUST 2021

Areas Covered



- Introduction
- Conceptual Definitions
- Overview
- Enterprise-Wide Risk Management
- Corporate Governance Risk
- Technology Risk

Introduction



Conceptual Definitions



What is Risk?

The effect of uncertainty on objectives (ISO 31000)

Its Anything that may affect the achievement of an Organization's objectives.

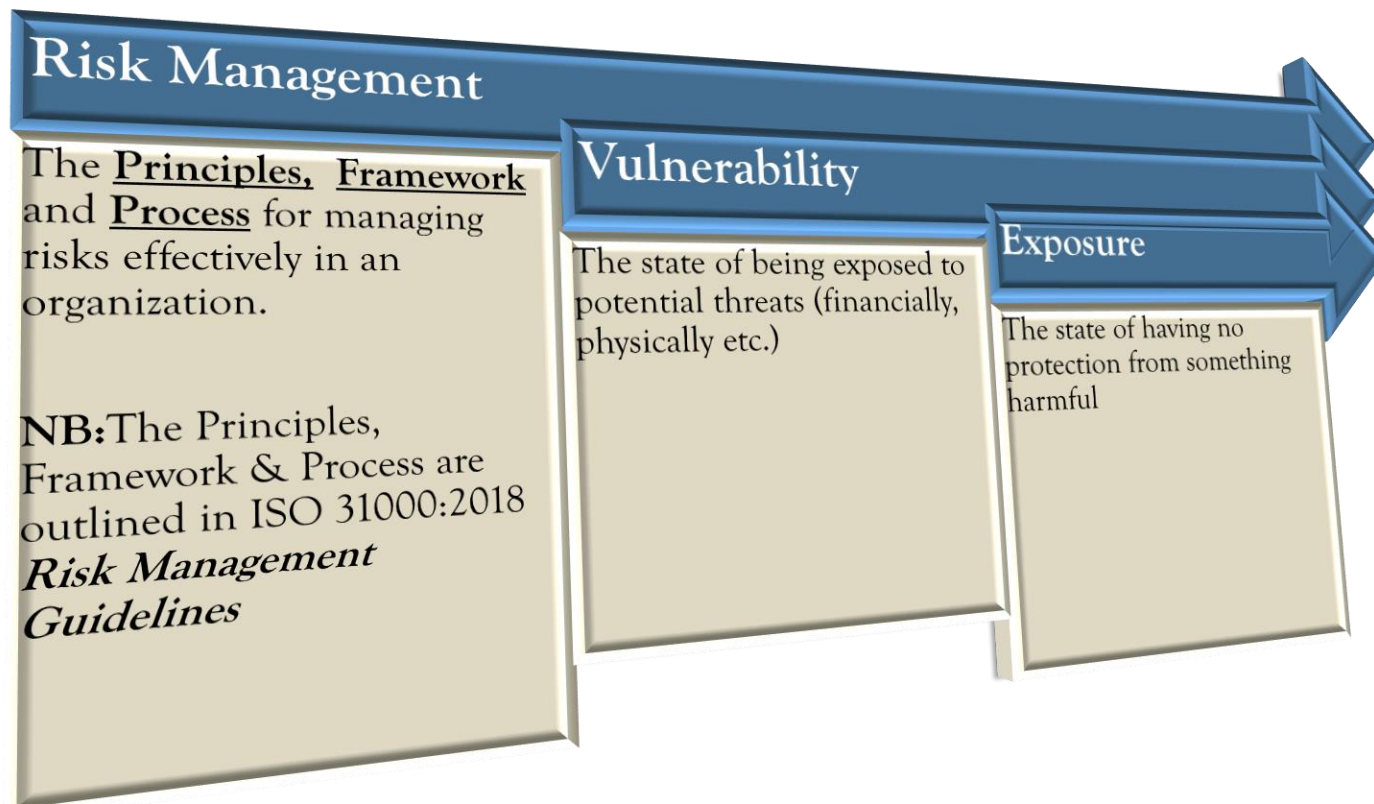
An effect

A deviation from the expected – positive and/or negative

Uncertainty

Situations under which either the outcomes and /or their probabilities of occurrences are unknown.

Conceptual Definitions Cont..



Conceptual Definitions



Threat

A person or anything likely to cause damage or danger

Risk Mitigation

The actions that must be taken to lower the likelihood of the risk occurring and/or to minimize the impact if the risk did occur.

NB: Risk can never be totally eliminated, but it can be mitigated to lessen its *likelihood* and or *impact*;

Conceptual Definitions



Risk responses

The means by which an organization elects to manage individual risks.

The main categories are:

To *tolerate the risk*;

To *treat it* by reducing its impact or likelihood;

To *transfer* it to another organization or

To *terminate* the activity creating it.

NB: Internal controls are one way of treating a risk;

Conceptual Definitions



Internal Controls

The processes, policies and procedures we use to govern the Organization's work, or any additional mitigating actions that we take to deal with a particular, or potential situation;

Risk Identification

The process of determining what might have happened, how, when and why;

Risk Analysis

Assessment of the *Likelihood* and *impact* of the risk on our goals and objectives

Conceptual Definitions



Risk Evaluation

The process of comparing the significance of the risks to define the order in which they should be dealt with;

Risk Treatment

The process of selection and implementation of measures to modify risk

The Enterprise Risk Management



What is ERM?

COSO defines ERM as:

“A process effected by an entities board of directors, management and other personnel, *applied in strategy setting and across the enterprise*, designed to identify potential events that may affect the entity, and help manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievements of entity objectives.”

Background and Overview of ERM



Although the concept of enterprise risk management (ERM) has existed for several years, it wasn't until the 2008 financial crisis that ERM gained significant prominence as an integral component of an institution's overall business strategy.

All organizations are taking a greater interest and adopting a proactive approach to risk and enterprise risk management to achieve the business objectives.

Views from the World Economic Forum (WEF)




The WEF-Annual Global Risks Reports

- The World Economic Forum (WEF) has commented on the increasing volatility, uncertainty, complexity and ambiguity of the world
- WEF states that:
The current competitive landscape can be defined by one word: *'disruption'*.
- The ideas of incremental progress, continuous improvement, and process optimizations do not work anymore.
- Organizations and board members need to be more adaptive to change. They need to think strategically about how to manage the increasing volatility, uncertainty, complexity and ambiguity of the world.
- WEF supports the analysis that stakeholders are more engaged today, seeking greater transparency and accountability for managing the impact of risk, while also critically evaluating leadership ability to embrace opportunities.

Why Enterprise-Wide Risk Management is Gaining Popularity



- 
1. Organizations no longer want to find themselves in a position whereby unexpected events cause financial loss, disruption to normal operations, damage to reputation and loss of market presence
 2. Stakeholders now expect that organizations will take full account of the risks that may cause non-compliance with statutory obligations; disruption and inefficiency within operations; late delivery of projects; or failure to deliver promised strategy.
 3. Companies are recognizing the need to deal with the totality of risk in relation to how they manage their business, moving from reacting to risk to a more proactive approach.

Effective Implementation of a Robust ERM

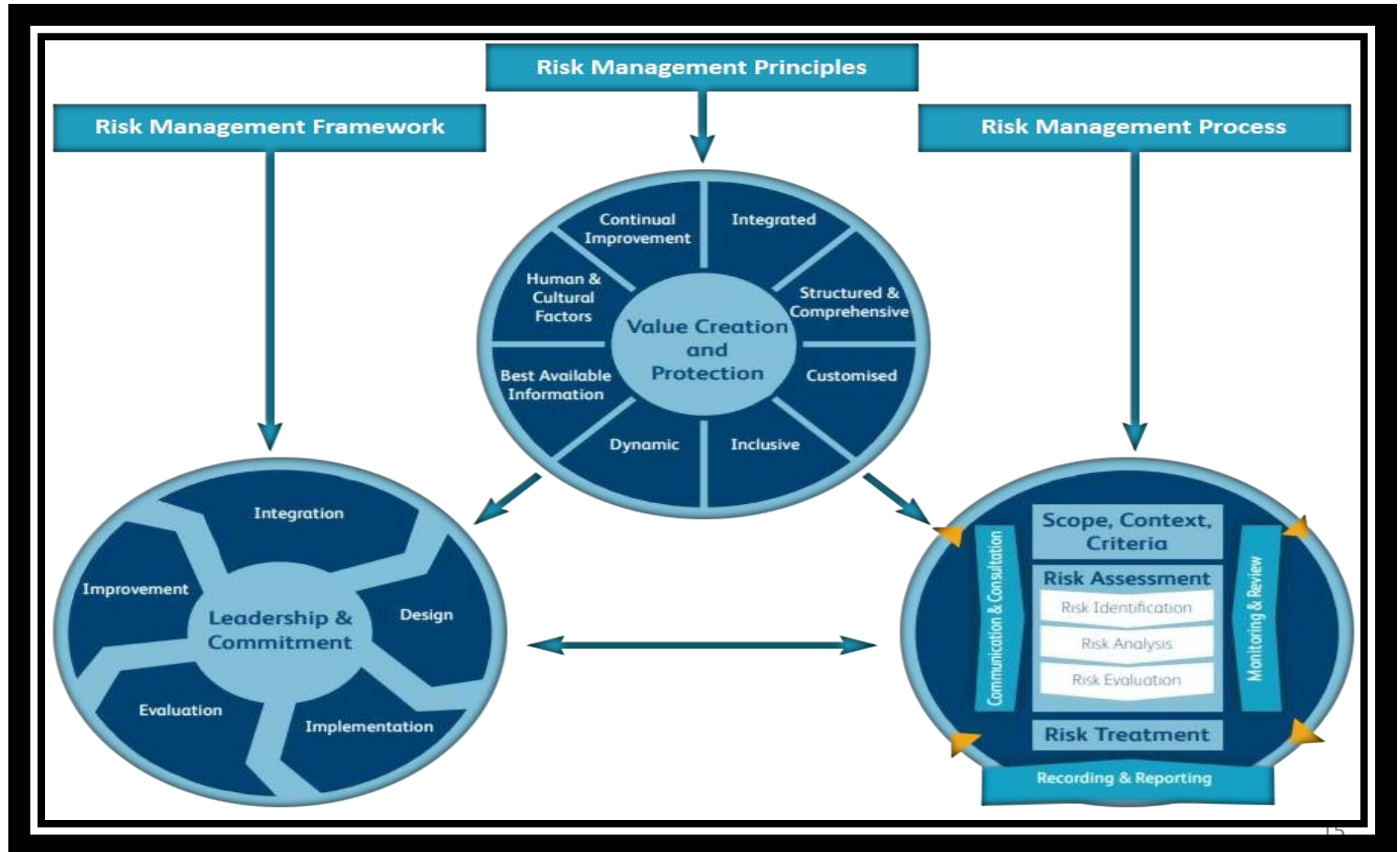


According to ISO 31000, managing risk is based on the principles, framework and process described in the guidelines (Current Version ISO 31000:2018).

These guidelines need to be adopted or improved so that managing risk is efficient, effective, and consistent within Organizations.

This combination of *Principles, Framework and Process* (ISO 31000) provides a high-level, but comprehensive, view of the components required to implement a robust ERM in any organisation

ISO 31000:2018 Components required to implement a robust ERM



ISO 31000:2018 Components Cont..



Principles

Principles include the requirement for the risk management initiative to be:

- i) Customized;
- ii) Inclusive;
- iii) Structured and comprehensive;
- iv) Integrated; and
- v) dynamic.

Framework

- i) The purpose of the risk management framework is to assist with integrating risk management into all activities and functions.
- ii) The effectiveness of risk management will depend on integration into governance and all other activities of the organisation, including decision-making.

The Process

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risks.

Historical and Current View of ERM



Historical View

Today

Hazard Risk Management	⇒ Enterprise Risk Management Operational, strategic, financial reputation and insurable risks
Focus on preservation of tangible assets	⇒ Recognition of the value of tangible and intangible assets
Silo approach: Each department / function	⇒ Holistic approach: Coordinated at the highest level
Risk management = separate function	⇒ Risk management is a corporate wide daily concern and is embedded in the operations
Risks are threats: Focused on avoidance of negative events	⇒ Risks can be threats and opportunities

An Effective Structure of ERM for All Institutions



Credibility Professionalism Accountability

An Effective Structure of ERM for All Institutions Cont....



An Effective Structure of ERM for All Institutions Cont....



Risk Management System

A comprehensive risk management strategy.

Ensure proper allocation of responsibilities for dealing with risk across the business.

A clearly defined risk appetite approved by the board

A written process defining the board approval required for any deviations from the risk management strategy or the risk appetite.

Appropriate written policies that include a definition and categorization of foreseeable and relevant material risks.

Suitable processes and tools (including, where appropriate, models) for identifying, assessing, monitoring, managing, and reporting on risks.

Regular reviews of the risk management system.

An Effective Structure of ERM for All Institutions Cont....



Risk Mitigation and Control

Controls to provide assurance over the accuracy and completeness of financial records.

Controls for other key business processes.

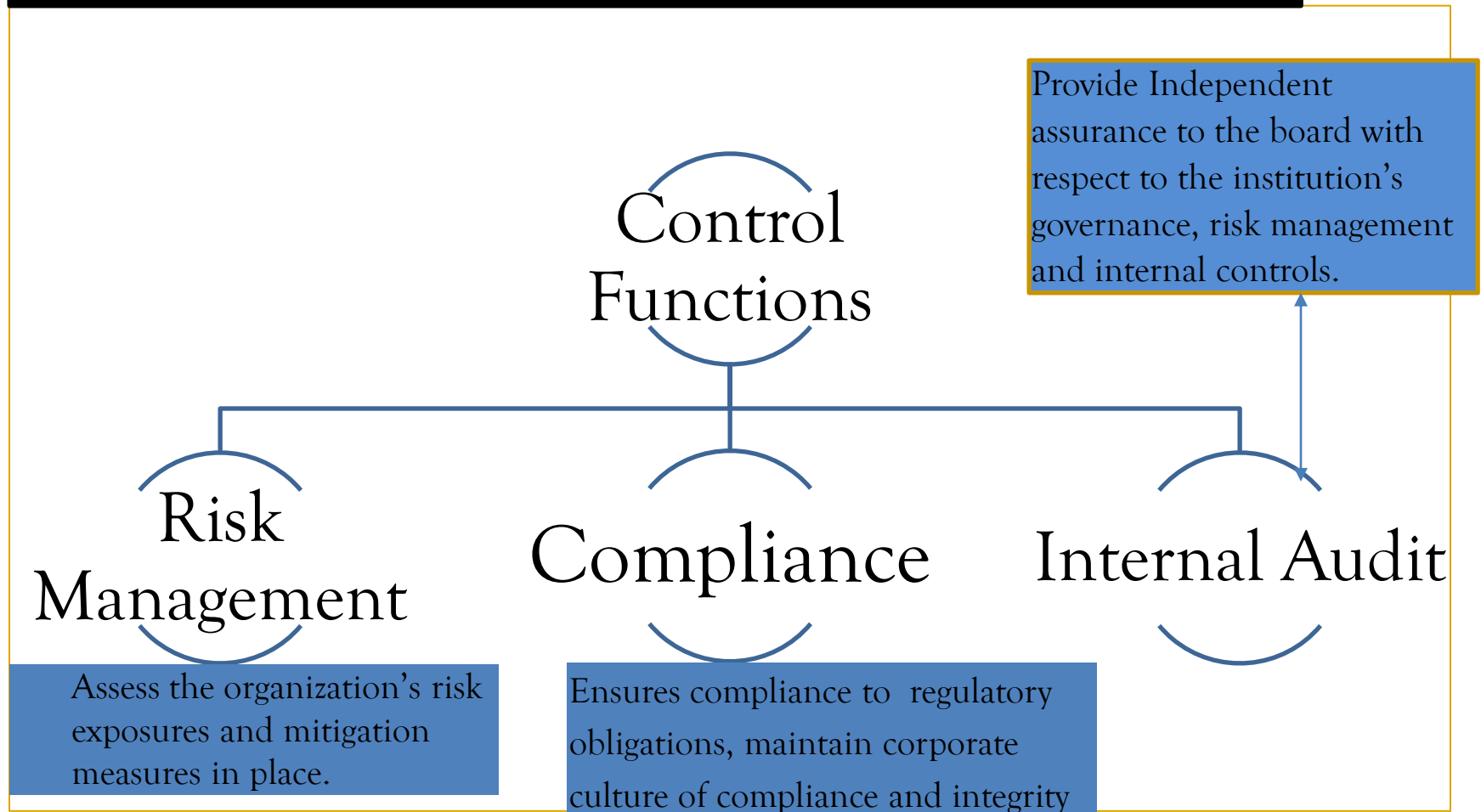
Appropriate segregation of duties.

A system of clearly defined management responsibilities and accountabilities.

A centralized written inventory of firm-wide key processes and policies.

Periodic testing and assessments (carried out by objective parties such as an internal or external auditor).

An Effective Structure of ERM for All Institutions Cont....



An Effective Structure of ERM for All Institutions Cont....



Risk Management Principles

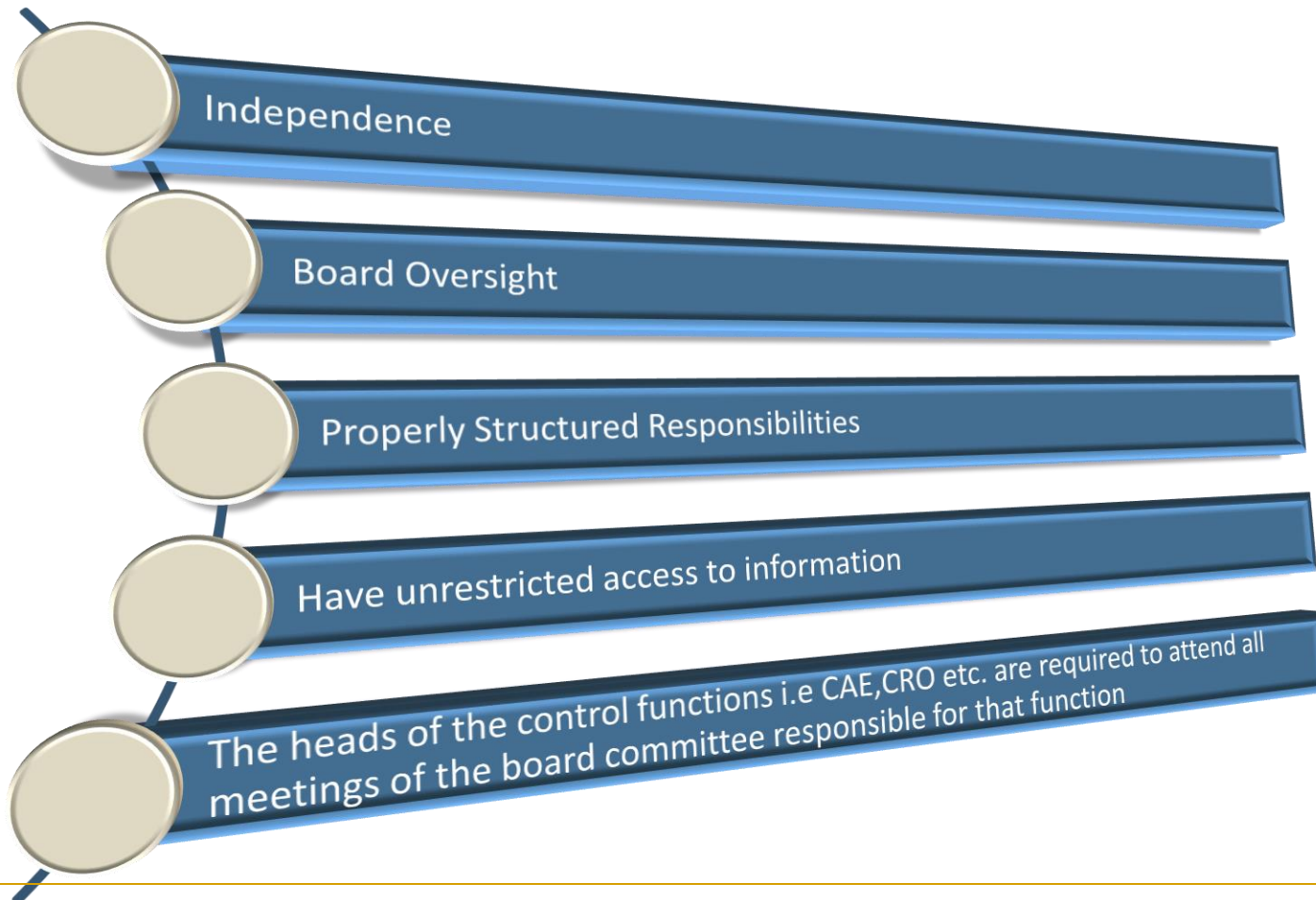
Principles include the requirement for the risk management initiative to be:

- i) Customized;
- ii) Inclusive;
- iii) Structured and comprehensive;
- iv) Integrated; and
- v) Dynamic (ISO 31000:2018)

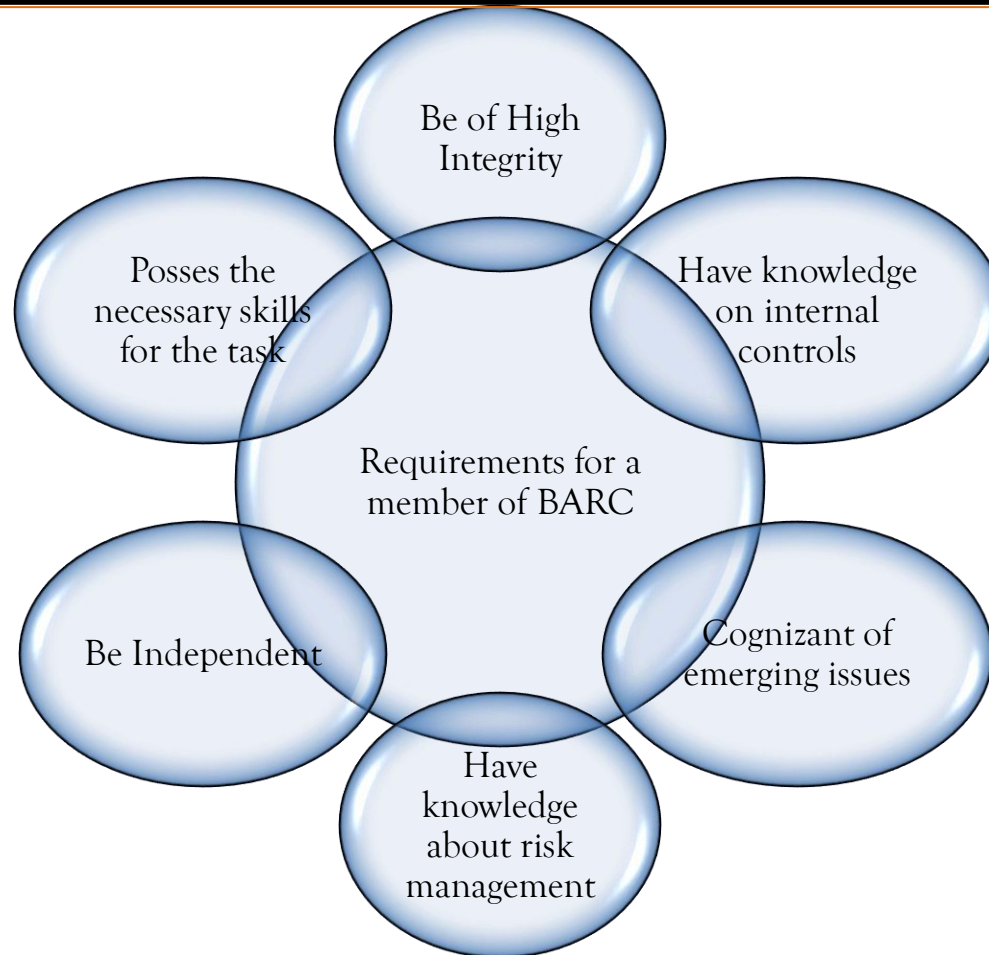
The Risk Management Process

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

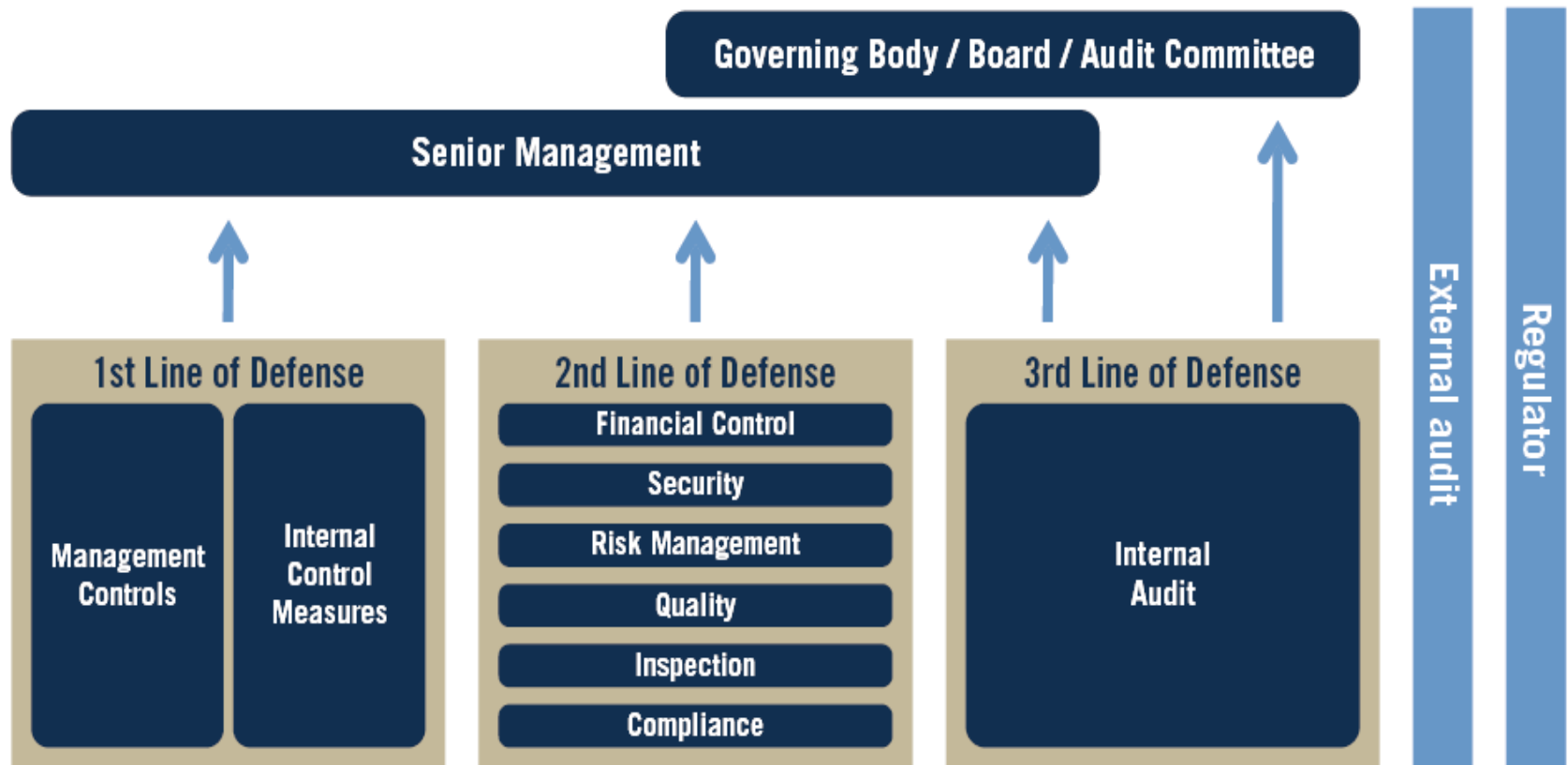
The Main Requirements for Control Functions



The BARC Oversight role



The IIA's Three Lines of Defense Model for Managing Risk



Benefits of Effective Risk Management



Supply Chain Resilience
Reduces Downtime
Optimize Customer Experience
Operational Excellence
Compliance Management
Reputation Management

Image Interpretations



Enterprise-Wide Risk Management 2021 Challenges and Opportunities



Challenges: We Must Avoid the Questions

Where was Internal
Audit/Risk
Management, especially
with no shortage of
high-risk areas?

Why didn't the
organization anticipate
“that risk” that kept us
from achieving the
strategic plan and key
performance goals?

Enterprise-Wide Risk Management 2021 Challenges and Opportunities



Opportunities:

Demonstrate the value IA
(and you) bring to the
organization

As agents of change to
provide insight and foresight
on the things that matter
most to achievement of the
strategic plan and key
performance goals of your
organization.

Key Considerations Regarding ERM



Three Initial Things to Consider Regarding ERM

Start with comprehensive audits of ERM and Business Continuity Processes, including benchmarking to frame recommendations for improvement.

NB:IA must have the skills, tools, and resources to audit ERM and key risks

Discuss risk management, emerging risks, risk appetite, changes in regulations, fraud, organization culture, etc.

Do you have the right skills and expertise? If not, make sure you regularly (not just annually) discuss the shortfall with Management/Audit Committee.

NB:Conduct regular discussions with Management/Audit Committee beyond IA findings.

NB:Read ERM White Papers

Key ERM Challenges faced by organizations in its successful implementation



2021 Key findings on ERM Practices within Organizations



Risks are not sufficiently incorporated into strategic planning.

Risk management consideration during strategy execution is also insufficient.

Organizations have an unacceptable exposure to third party risks.

Business continuity plans don't help deal with unexpected events (Covid-19 scenario)

Organizations detect risks too late (corporate failures i.e retail)

Organizations are ill prepared to manage the risks of business model changes post pandemic

2021 Key findings on ERM Practices within Organizations



Risk managers feel least able to tackle culture as a risk area..

Risk managers are concerned that organizations are making large, risky changes after COVID, in terms of the business model and cost management..

Risk managers are concerned about decisions being taken outside of risk appetite.

Way forward for Organizations to Ensure effectiveness of ERM



There is no one size fits all approach, but organizations must

1. Agree on risk appetite and ensure it is defined for all major risk areas, determining what is acceptable risk/reward

2. Ensure the organization's culture aligns with their appetite

3. Develop effective continuous monitoring tools for agreed to and emerging risks

Way forward for Organizations to Ensure effectiveness of ERM cont...



There is no one size fits all approach, but organizations must

4. Provide the proper assurance and ensure disclosures are transparent

5. Have Board support that is visible in word and speaks on the importance of risk management.

6. Wholly integrate risk management into business planning and strategic decision making

Way forward for Organizations to Ensure effectiveness of ERM cont...



There is no one size fits all approach, but organizations must

7.Align desired behaviors with performance and incentives.

8.Embed early warning systems for timely awareness of changes in control effectiveness and risk.

Key Aspects to an ERM Audit



Ascertain how management and the Board determine risk appetite; how is that communicated?

Determine how the top risks get incorporated into

- i) The organization's strategic plan and goals and objectives for each function
- ii) Determine if the organizations incentive programs are aligned with the above
- iii) Evaluate oversight over third parties and the risks that can keep you from achieving the plan.

Examine how management and the Board determine top risks; how is that communicated?

- Determine what dashboards have been created to monitor identified risks

Determine how management monitors emerging risks

Evaluate how well ERM is understood across the enterprise and how it impacts culture

Evaluate the impact of business process changes as a result of the pandemic or technology

Emerging issues Across the Globe that are Increasing Risks



A pandemic
(Covid-19) that
doesn't seem to
end leading to

- ✓ High country debt levels, displaced workers, growing inequality, lost trust etc.
- ✓ Countries lacking more financial flexibility and increasing business taxes
- ✓ Change in how and where we work; talent shortage/issues

Political turmoil
– U.S., China,
Russia, the
Middle East, etc.

Climate change
continues to
impact global
operations
(Case of Haiti)

Global supply
chain shortages

- ✓ China dominating in acquiring access to key elements across the globe

Emerging issues Across the Globe that are Increasing Risks



Cyber issues
growing daily

Digitalization
and business
transformation

Technological
innovations like
Uber,
ecommerce are
disrupting
business models

Rising interest
rates, impact
on
government
debt,
businesses,
and
consumers.

Increased
Focus on
Government
regulations

- Data privacy
issues as well as
their impact
from cyber
intrusions

Emerging issues Across the Globe that are Increasing Risks



Corporate Frauds are still at the forefront of issues to address

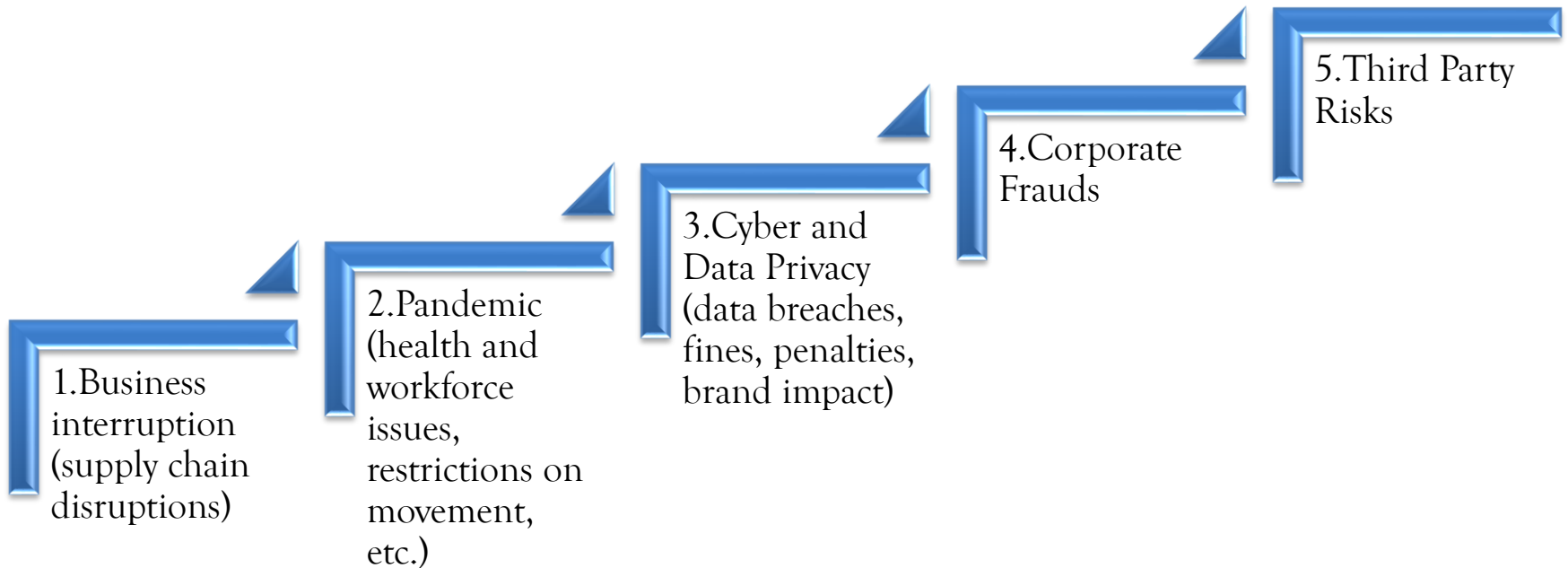
Ability to timely identify emerging risks

Inability to use data analytics to achieve market intelligence or productivity gains.

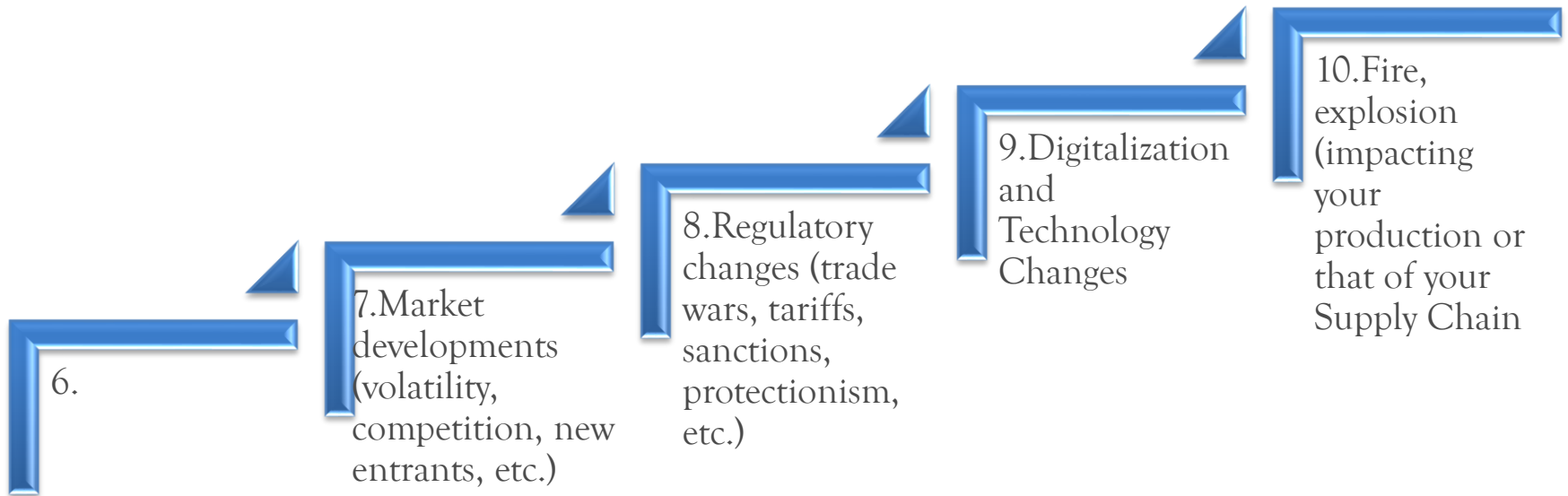
Resistance to change coupled with inability to adjust ops and IT infrastructure.

- Agility and ability to quickly adapt to business transformation

Top Ten Business Risks for 2021 to be addressed by organizations



Top Ten Business Risks for 2021 to be addressed by organizations cont..



Top Ten Business Risks for 2021 to be addressed by organizations



11. Macroeconomic issues (monetary policy, commodity price increases, inflation, etc.)

12. Climate change & natural calamities (storms, floods, wildfires, earthquake, hurricane, etc.).

13. Political risks and violence (political instability, war, terrorism, riots, etc.)

THE BIG QUESTIONS



Is Your Internal Audit Team Addressing Key Risks?

1. Have you benchmarked and audited your organization's ERM process?

2. Are you Ensuring the organization has a system to track changes in risks and monitor for emerging risks?

3. Have you assessed if you have adequate skills, expertise, resources, and relevant knowledge to audit key risks?

THE BIG QUESTIONS



4. Have you assessed if you have adequate skills, expertise, resources, and relevant knowledge to audit key risks?

5. Do you have regular discussions with Management/Audit Committee on the key risks, emerging risks, leading practices, cyber, regulatory changes, fraud, etc. and the role IA plays auditing such?

6. Do you incorporate ERM considerations into every audit?

7. Are you doing enough with respect to cyber, third-party risks, and business changes as a result of the pandemic or disruptive technologies?

What Is Corporate Governance?

Corporate governance is the system of rules, practices, and processes by which a firm is directed and controlled.

It essentially involves balancing the interests of a company's many stakeholders, such as shareholders, senior management executives, customers, suppliers, financiers, the government, and the community.

Corporate Governance Overview



Corporate governance is the structure of rules, practices, and processes used to direct and manage a company.

A company's board of directors is the primary force influencing corporate governance.

Bad corporate governance can cast doubt on a company's operations and its ultimate profitability.

Corporate governance entails the areas of environmental awareness, ethical behavior, corporate strategy, compensation, and risk management.

The basic principles of corporate governance are accountability, transparency, fairness, and responsibility.

Key Consideration of Good Corporate Governance



A board of directors should consist of a diverse group of individuals, those that have skills and knowledge of the business, as well as those who can bring a fresh perspective from outside of the company and industry

The board of directors must ensure that the company's corporate governance policies incorporate the corporate strategy, risk management, accountability, transparency, and ethical business practices.

A transparent set of rules and controls in which shareholders, directors, and officers have aligned incentives.

Proper Board composition, diversity, and refreshment, and leadership structure

Shareholder and stakeholder engagement is robust (Stakeholder issues are addressed)

Good governance practices and ethical corporate culture is implemented

Long-term strategy, corporate purpose, and sustainability issues are considered

Corporate Governance Risks



What are
Corporate
Governance Risks?

These are risks that relate to directors' decisions regarding Board leadership, composition and structure; director and CEO selection; CEO compensation and succession and other important governance matters critical to the enterprise's success.

Risks Inherent in Corporate Governance Process



Bad corporate governance can cast doubt on a company's reliability, integrity, or obligation to shareholders; all of which can have implications on the firm's financial health.

Tolerance or support of illegal activities can create scandals (like the one that rocked Volkswagen AG starting in September 2015) and possible legal suits

Reputational damage to the company resulting from support of unethical business practices

Conflict of interest among the Board Members leading to reputational and financial consequences to the company

Evaluation Checklist for a Good Corporate Governance



Disclosure practices

Executive compensation structure (is it tied only to performance or other metrics?)

Risk management (what are the checks and balances of making decisions in the company?)

Policies and procedures on reconciling conflicts of interest (how does a company approach business decisions that might conflict with its mission statement?),

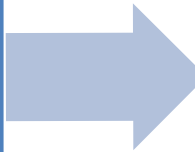
The members of the board of the directors (do they have a stake in profits?),

Contractual and social obligations (how do they approach areas such as climate change?)

Complaints received from shareholders and how they were addressed

Audits (how often are internal and external audits conducted and how have issues been handled?)

What is
Strategic
Risk?



Strategic risk is the current and prospective impact on the company's strategic Objectives arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes.

ii) It is a risk that could significantly impact on the achievement of the institution's vision and strategic objectives as documented in the strategic plan.

iii) Strategic risks are most consequential to the organization's ability to execute its strategy and achieve its objectives. They entail the risk exposures that can ultimately impact shareholder value or even threaten the business's survival.

Strategic Risk Assessment Checklist



Understand the strategies of the organization



Collect data and views on strategic risks from the organization



Prepare a preliminary strategic risk profile



Validate and finalize the strategic risk profile with management and the Board



Develop a strategic risk management action plan



Communicate the strategic risk profile and action plan



Implement the enterprise risk management action plan

Technology Risk



What is Technology Risk?

Technology risk refers to any risk of financial loss, disruption, or damage to the reputation of an organisation as a result of the failure of its information technology systems (i.e Cyber risk is a subset of technology risk)

Key Points

- a) Information technology or IT risk is basically any threat to your business data, critical systems, and business processes.
- b) It is the risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an organisation.

Most Common Technology Security Risks you need to avoid.



Phishing

Phishing is the use of fraudulent emails or phone calls to get sensitive information, such as bank account numbers, credit card information or passwords.

NB: It's a type of **social engineering**, (an attack that uses misrepresentation to get sensitive information)

Pretexting

Pretexting involves the creation of a fake identity or scenario to fool a person into disclosing information.

NB: fraudster may email or call your company claiming to be a supplier, survey firm, govt inspector or insurance company to get sensitive data.

NB: A pretext attacker could also pose as a computer technician responding to a call for service to access your network.

Malware

Malicious software (or "malware") is any software that has a harmful intent. It may steal or corrupt your business information, cause systems to fail or secretly record your computer activity. Malware typically infects a computer following a phishing attack or an employee accidentally downloading infected files.

Ransomware is software that blocks access to computers or files until a ransom is paid. In May 2017, a massive ransomware attack affected more than 100,000 organizations in at least 150 countries, costing billions of dollars.

Most Common Technology Security Risks you need to avoid cont..



Wi-Fi and remote work

A poorly secured Wi-Fi system can leave your business vulnerable to a hacker within range of your network. A hacker could gain sensitive information, damage your systems or install ransomware.

If you access your business network remotely through an unsecure server, others could see your traffic and access your system.

In a public area, you can be at risk if you go online through a “spoofed” Internet server—one set up to appear to be a legitimate Wi-Fi connection. Accessing the Internet via such a machine gives an attacker access to your system and possibly your business network.

Also be alert when working outside the office. Information can be compromised if you’re working on a train or plane or in a café, allowing a stranger to read what’s on your screen.

Outsourced IT services

While many cloud service providers have good Internet security, not all of them do. You can be at risk if the provider has poor security, leaving your data vulnerable to an attack.

If the provider suffers an attack, you may also be liable for compromises of customer data.

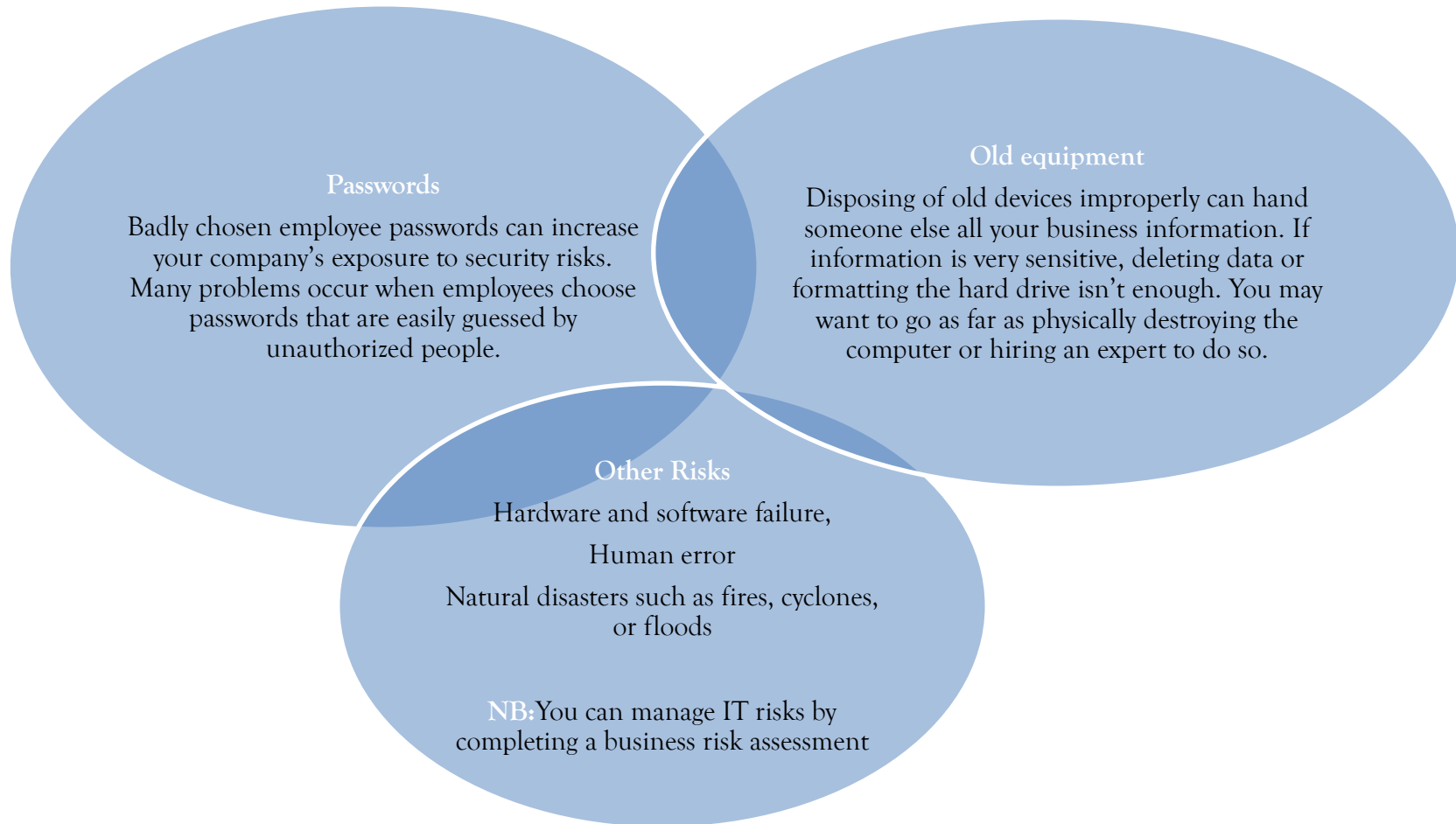
Businesses face similar risks if they contract outside technicians to service their IT needs. You could be vulnerable if IT personnel have poor training or don’t follow best practices.

Online pop-ups

Malware can infect computers through a “pop-up” that appears while you’re browsing the Internet. A pop-up is a window that opens when you visit a website.

Most pop-ups are legitimate, but in some cases clicking on them can initiate a download of ransomware or a virus.

Most Common Technology Security Risks you need to avoid cont..



The Purpose of IT Risk Assessment. Why Bother?

IT risk assessment is the process of identifying security risks and assessing the threat they pose. The ultimate purpose of IT risk assessment is to mitigate risks to prevent security incidents and compliance failures.

Components of an IT Risk Assessment



An IT risk assessment starts with risk intelligence and threat analysis.

You need to make three lists:

1. The IT assets in your organization and how much damage their loss or exposure would cause

2. The business processes that depend on those assets

3. The threat events that could impact those assets and how likely those events are

Benefits of IT Risk Assessment



Understanding Your Risk Profile (to help prioritize risk management tasks and allocate resources appropriately)

Identifying and Remediating Vulnerabilities (determine the best steps for improving your information security.)

Inventorying IT and Data Assets (With a complete, up-to-date inventory from your IT risk assessment, you can determine how to protect your most critical software and data assets)

Mitigating Costs (Regular IT risk assessment can help your company eliminate unnecessary security spending)

Complying with Legal Requirements (Most organizations must comply with the privacy and data security requirements of various regulations. Any company that does business with European residents, for example, has to regularly evaluate their risk to comply with the GDPR (

Key Controls to Mitigate IT Risks



ICT GOVERNANCE

(aids in aligning IT with the company goals and strategy and mitigating the inherent ICT risks)

(i.e CTO reporting to the Board, ICT Policy manual, ICT Risk Register and ICT Strategic Plan)

• CHANGE MANAGEMENT

IT Change Management is a formal set of procedures and steps that are set in place to manage all changes, updates, or modifications to hardware and software (systems) across an organization

• LOGICAL AND PHYSICAL ACCESS CONTROLS

i) Access controls are critical to restrict access to company data, IT assets and programs by means of preventing unauthorized access or changes, including prevention of unintentional errors and fraud by employees and/or intruders

ii) . Physical access control limits access to company premises where IT resources are kept and physical IT assets

iii) Logical access control on the other hand limits connections to computer networks, system files and data i.e firewalls

PHYSICAL & ENVIRONMENTAL SECURITY

various measures or controls that protect a company from loss of connectivity and availability of computer processing caused by theft, fire, flood, intentional destruction, unintentional damage, mechanical equipment failure and power failures.

Buildings that host IT facilities must have appropriate control mechanisms in place for the type of information and equipment that is stored there.

i.e system alarms, Temperature controls, Window & Door Locks, A Server room locked with a card access system installation, Server room fire extinguishers, raised floors etc)

• BACKUPS AND RECOVERY

In order to ensure that normal business operations can continue following a disaster or a complete system failure, Disaster Recovery and Contingency plans should be put in place and regularly reviewed and tested.

Key Controls to Mitigate IT Risks



INFORMATION SECURITY CONTROLS

Information security involves applying security controls to prevent unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of company's sensitive information

Information Security is critical in reducing the risk of data breaches and attacks in the company's IT systems and networks by outsiders. This will preserve the confidentiality, integrity and availability of the company's information and data

- i) Firewalls should be used to protect the network perimeter from suspicious activities
- ii) Antivirus software should be used to prevent damage from viruses
- iii) Incoming and outgoing data traffic are monitored 24/7 to identify potential phishing attacks, DDoS attacks and other attempts to penetrate the network perimeter.
- iv) Penetration testing should be performed twice annually to test for vulnerabilities

• ICT INCIDENT MANAGEMENT

Incident management (IM) is an IT service management (ITSM) process area that functions to restore a normal service operation as quickly as possible and to minimize the impact on business operations.

Incident management in ICT is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An effective Incident management system should restore services quickly after a major interruption. The incident response process should be documented and used regularly when responding to abnormal situations

• THIRD-PARTY SYSTEMS RISKS AND CONTROLS

Third-party security involves checking and ensuring that third parties such as business partners, suppliers and vendors maintain an acceptable level of cybersecurity so that they can safely do business with the company (Sign SLAs, BCPs, ERP, Cyber Security Plan)

Key Controls to Mitigate IT Risks



LOGICAL SECURITY CONTROLS

These consists of software safeguards for an organization's systems, including user identification and password access, authenticating access rights and authority levels.

. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation.

- 1.New employees are provided access to system resources after being approved by Human Resources,
- 2.Terminated employees have their access credentials deleted within 15 minutes of notification by HR to the IT department.,
- 3.Users access matrix is reviewed periodically i.e quarterly, Activities of the Users are reviewed, and any anomaly investigated

Key Controls to Mitigate IT Risks



**If you don't invest in risk management,
it doesn't matter what business you're
in, it's a risky business.**

Gary Cohn

quotezancy

THE END



THANK YOU